UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA **22-CR-6009 (CJS)**

v. **ATTORNEY AFFIDAVIT**

JOHN DOUGLAS LOONEY
Defendant.

James A. Napier, Esq, deposes and says:

1. The USA v Corbett spreadsheet which we included in our motion was provided by a lawyer, Thomas D. Church, (Pate, Johnson & Church , Atlanta Georgia), who litigated the case. We have included all the information we have on this case as Exhibits.

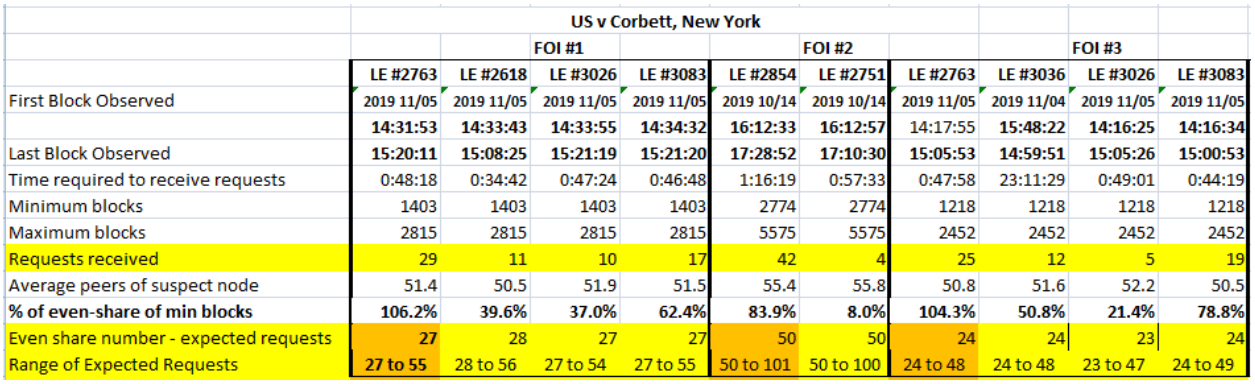
Ex. A	The Affidavit USAO_000004-000033
Ex. B	The spread sheet data USAO_000034-000034
Ex. C	Officer's notes USAO_000035-000036
Ex. D	Levine paper USAO_000039-000

2. The data from the USA v Corbett 20CR525 SDNY case shows that requests are distributed unevenly, not by even share, and we find the Corbett data proves conclusively that the Levine Formula, the basis for even share, does not work. This data collected by the FBI in Corbett shows multiple FBI nodes, 4 for FOI 1, each receiving a different share of requests that are not roughly even, such that one node identifies the downloader and three indicate a relayer proves the methodology is false. Each node is operating independently, and the prosecution claims that a factor of 10 or fewer requests than even share could still indicate a downloader, however not one of these 3 government nodes identified a downloader. The result is a 75% false positive. This is an actual case and no assumptions are required as is the case with the Levine Formula.

3. This is significant and proves the government methodology is false with an actual real case. We have provided with this document additional evidence showing the government is using a false method to achieve probable cause for search warrants. However, based upon the importance of the Corbett case, we respectfully request an additional three to four weeks time to allow us to find additional cases where multiple FBI nodes were involved in the data collection, and also to allow us time to acquire a Freenet developer to testify or provide an affidavit. In Corbett there were 7 separate, independent, FBI nodes colleting and logging data, and we believe there must be more cases like this within the US. We are currently talking to lawyers in Georgia, Wisconsin, and Ohio, who also have Freenet cases. We fully believe that this is not an isolated case, and assume this is not a unique occurrence within the United States.
4. We do not believe the magistrate saw the spreadsheet in this case showing the multiple FBI nodes. There is no mention of the multiple FBI nodes in the affidavit, and there was also no mention of multiple FBI nodes in the Officer's notes, both included in the Exhibits as A and C. The affidavit in this case only describes the data from one FBI node for the three FOI's,
5. The government has clearly stated that the modified Freenet software is identical to normal Freenet software except for the logging function, so there is no communication between the FBI nodes other than normal Freenet traffic. Each of the FBI nodes in this case is independent from the other FBI nodes, and the government has not stated that in the case of multiple FBI nodes monitoring the same suspect that only one node would be used to identify the downloader. As far as we know, they have never suggested that a situation such as seen in Corbett exists.
6. Now if we look at the data for Corbett, File of Interest #1, we have 4 separate FBI nodes each connected to the same suspect (IP 108.30.166.37), at roughly the same time. This means that each FBI node is operating independently and if we refer to Officer Turner's Figure 1 in the affidavit, we have the suspect node A connected to the FBI nodes as B, C, D, and E. The Prosecution stated that the 'Pass' at the bottom of a column indicated that this node A (IP 108.30.166.37) is the downloader, identified by LE #2763 But we have two problems; first, according to Officer Turner's description Freenet operates by taking the number of blocks required (1403) and dividing by the number of peers then evenly sharing with each peer. This means that each peer, including all 4 FBI nodes would be sent 1403/51.3=27 requests. It is clear that the FBI nodes did not receive roughly even shares since the results were 29, 11, 10, and 17. So there was no even share. This is not a test but actual real results based upon data

collected in the field. There are <u>no assumptions</u> here, other than all the peers were active and communicating during the test.

7. The data collected in this case offers <u>objective</u> <u>materially relevant proof</u> that Freenet does not use even share, and Levine's model is wrong.



	US v Corbett, New York									
	FOI #1				FOI #2		FOI #3			
	LE #2763	LE #2618	LE #3026	LE #3083	LE #2854	LE #2751	LE #2763	LE #3036	LE #3026	LE #3083
First Block Observed	2019 11/05	2019 11/05	2019 11/05	2019 11/05	2019 10/14	2019 10/14	2019 11/05	2019 11/04	2019 11/05	2019 11/05
	14:31:53	**14:33:43**	**14:33:55**	**14:34:32**	**16:12:33**	**16:12:57**	14:17:55	**15:48:22**	**14:16:25**	**14:16:34**
Last Block Observed	**15:20:11**	**15:08:25**	**15:21:19**	**15:21:20**	**17:28:52**	**17:10:30**	**15:05:53**	**14:59:51**	**15:05:26**	**15:00:53**
Time required to receive requests	0:48:18	0:34:42	0:47:24	0:46:48	1:16:19	0:57:33	0:47:58	23:11:29	0:49:01	0:44:19
Minimum blocks	1403	1403	1403	1403	2774	2774	1218	1218	1218	1218
Maximum blocks	2815	2815	2815	2815	5575	5575	2452	2452	2452	2452
Requests received	29	11	10	17	42	4	25	12	5	19
Average peers of suspect node	51.4	50.5	51.9	51.5	55.4	55.8	50.8	51.6	52.2	50.5
% of even-share of min blocks	**106.2%**	**39.6%**	**37.0%**	**62.4%**	**83.9%**	**8.0%**	**104.3%**	**50.8%**	**21.4%**	**78.8%**
Even share number - expected requests	**27**	28	27	27	50	50	24	24	23	24
Range of Expected Requests	**27 to 55**	28 to 56	27 to 54	27 to 55	50 to 101	50 to 100	24 to 48	24 to 48	23 to 47	24 to 49

8. This data is taken from the FBI spreadsheet provided in the Corbett case, and is included in its original form as Exhibit B. We have added the bottom two rows using the government calculations used in the Looney case. The bottom row provides the expected number of requests that would be received by the FBI node from the downloader. The first FBI node observing the suspect for each FOI is within the range expected by even share. For FOI #1, FBI node LE #2763 received 29 requests, and per the Levine methodology, a node receiving requests in the range from 27 to 55 would be a downloader. This was flagged as a downloader in the Affidavit in this case. The other three FBI nodes did not receive the number of requests within the range, and did not flag the suspect as the downloader. So one FBI node says suspect is downloader and three do not say suspect is downloader. This is with all four FBI nodes looking at the same suspect at the same time, getting different numbers of requests, and reaching different conclusions as to downloader or relayer.

9. This second problem is that the other three FBI nodes are not flagged as connected to a downloader, meaning that one peer identified the suspect as a downloader and three did not. This is a 75% false positive which according to Levine's test should be nearly impossible. Similar results are shown on the other two Files of Interest with 50% false positive on FOI #2 and 75% false positive on FOI #3.

10. The prosecution claimed that there could be a factor of 10 between a node directly connected and one that was two hops away, but this approach seems to be used to capture any case where the first level requests were less than the even share number. We do not agree with

this approach to determine the number of requests that would be received by a node two hops away, but in any case these FBI nodes did not identify the suspect as a downloader. It does not explain the suspect node sending a different number of requests to each node in the first place. This receipt of different numbers of requests fits perfectly with FOAF routing.

11. The government disclosed that the label "**pass**" which is shown at the bottom of each target summary and labeled as 'statistical test results' means that the Formula has identified the suspect node as a downloader. We note that the 'pass' is <u>not</u> shown for the other connected FBI nodes which would mean that the Formula did not identify the suspect as a downloader. The result then is that the Formula identified a downloader in one case and a relayer (not downloader) in three cases for FOI #1.

In conclusion, the requests received by the FBI nodes were not roughly even, and only the FBI node which received the most requests identified the downloader, three nodes did not identify for a 75% false positive. This factor of 10 issue was described in the Affidavit for the case herein at ¶44 to ¶51 as a method where a prediction is made of how many requests would be received by a node that was two hops from the downloader. Freenet does not divide the requests and this is not valid.

12. We have been in contact with a Freenet developer who was the author of the paper we provided with our motion: "The Discredited Levine 2017 Approach Is Still Used." The author is Dr. Arne Babenhauserheide, a Professor of Meteorology and Climatology at a prominent German University. He has extended the paper and provided an explanation of the Formula, the variables in the Formula, why the Formula is false, and provides an extended analysis and detailed breakdown of the Levine Formula in Exhibit F of this document. The paper attempts to provide answers to many of your questions more directly.
13. Dr. Arne Babenhauserheide has been one of the developers of Freenet for over 10 years. We would appreciate the extra time to allow us to convince this Freenet developer to testify or provide an affidavit. He is particularly reluctant because of the experience of another Freenet developer who had planned to testify for the defense in the Dickerman evidentiary hearing. Apparently his experience was particularly bad and resulted in him breaking off contact with the Freenet project. That developer was Steven Dougherty who traveled to St. Louis, but did not testify. When we asked about an affidavit, Dr Babenhauserheide response to us was *"You can explain this to the judge: no sane person would write an affidavit in these cases if they know the experience of Steve Dougherty, because getting into the US legal system heavily*

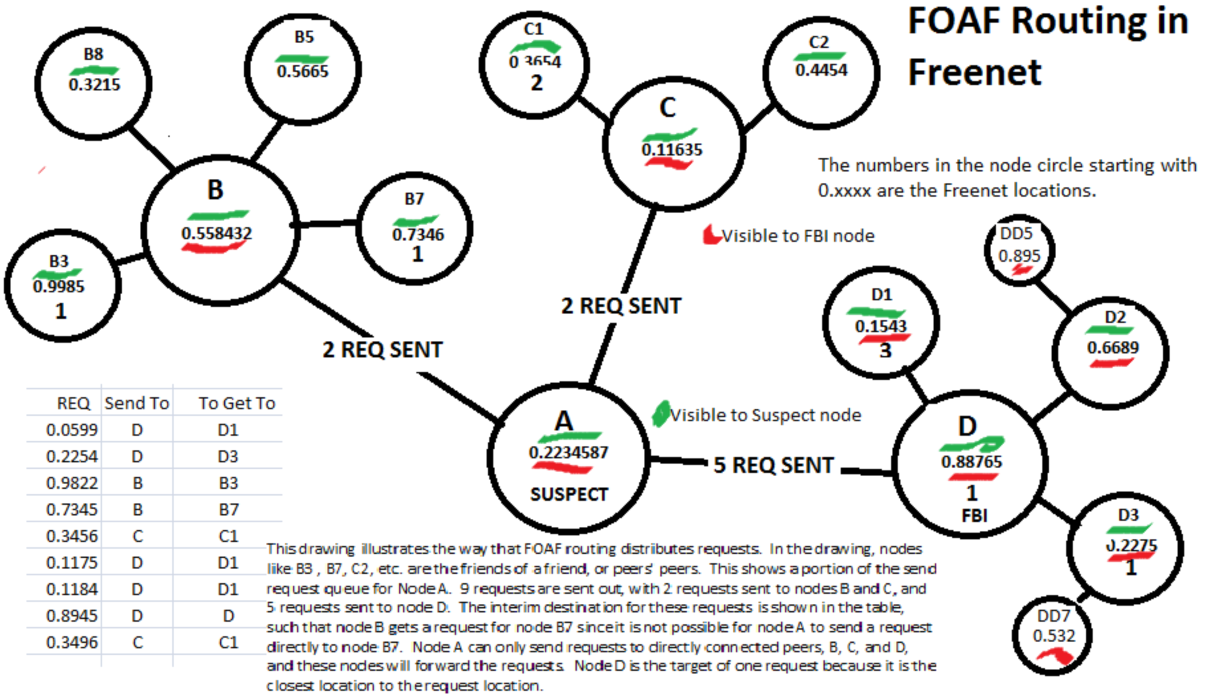
threatens their mental wellbeing." We are working to try and find details of what happened to Dougherty.

This is the Formula:

$$Pr(H1|r) = \frac{\frac{1}{g+1} B\left(r; T, {}^{1}/_{g}\right)}{\frac{1}{g+1} B\left(r; T, {}^{1}/_{g}\right) + \frac{g}{g+1} B\left(r; T, {}^{1}/_{gh}\right)}. \qquad (6)$$

14. Regarding this formula, apparently used by the government herein, Dr. Babenhauserheide states that because the two most influential variables (g and h) are wrong, the whole calculation is wrong. "*A correct formula would not use the number of peers for g and h*". This Freenet developer also states, "using 1/g and 1/gh in there is why they must assume that Freenet uses even share since Freenet does no (sic) use even share, there math is wrong and their whole calculation breaks apart."
15. This term, *Pr*(*H1*|r), is the probability that, based upon the number of requests received (r), the suspect is the downloader. For example, there is a 90% probability that the suspect is the downloader. A simple to understand answer that is not presented in either the Corbett or Looney case. This probability number is much easier to understand and explain than % of even share, or why a user who sends fewer than the number of even share requests is the downloader.
16. Neither the Formula nor the calculated probability is shown in the Affidavits for either case. The Formula is only referenced (¶52-¶54), as the basis for identifying the suspect as *"significantly more probable than not*" the downloader of a File of Interest. It is not clear why Officer Turner neglects to include this information about the Formula which is referenced 18 times. The Formula is not explained and we believe that it would be impossible for a lay person to plug the data into the Formula and verify the conclusions of Officer Turner.
17. Although the Formula is touted as providing, with 98% certainty, the identity of the downloader, we are never shown these probabilities, instead the number of requests received are simply compared to the even share number. The data from USA v Corbett conflicts with the claimed 98% certainty by showing a 75% false positive rate.
18. We are not aware of any test or verification by any independent authority to verify this key piece of the Affidavit which is used to reach the conclusions as to probable cause. We have provided an analysis of the Formula, Exhibit F, by a Freenet developer for over 10 years. This paper explains the terminology of the Formula, and where the Formula is wrong.

19. FOAF routing is important because it makes it impossible to predict the number of requests that would be received from a downloader, the basis for the government conclusions. With FOAF routing, the number of requests is a meaningless number. It is not necessary to understand the math shown in the various articles to understand why this works and why the number of requests cannot be determined. The drawing below has been shown before, but it shows FOAF routing more clearly than a simple description.



REQ	Send To	To Get To
0.0599	D	D1
0.2254	D	D3
0.9822	B	B3
0.7345	B	B7
0.3456	C	C1
0.1175	D	D1
0.1184	D	D1
0.8945	D	D
0.3496	C	C1

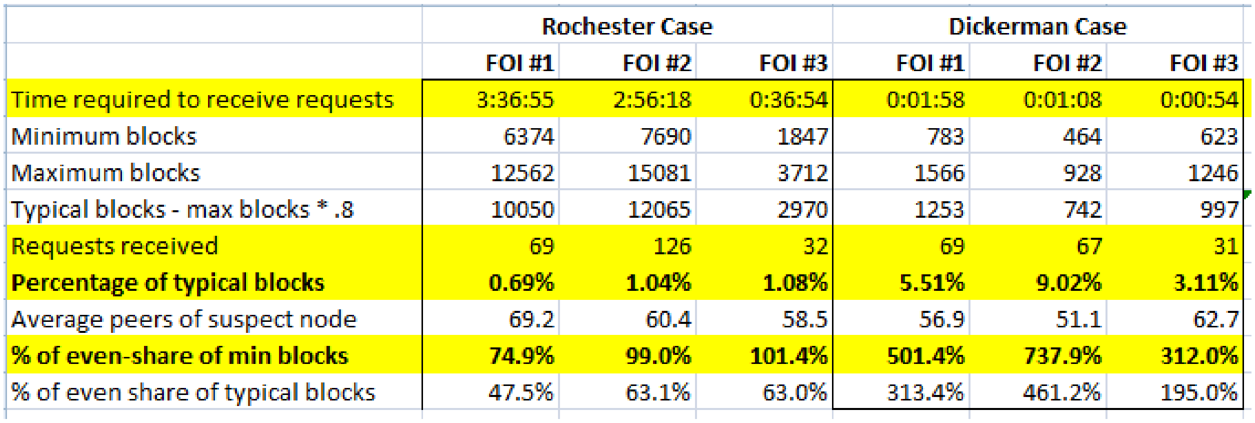
This drawing illustrates the way that FOAF routing distributes requests. In the drawing, nodes like B3 , B7, C2, etc. are the friends of a friend, or peers' peers. This shows a portion of the send request queue for Node A. 9 requests are sent out, with 2 requests sent to nodes B and C, and 5 requests sent to node D. The interim destination for these requests is shown in the table, such that node B gets a request for node B7 since it is not possible for node A to send a request directly to node B7. Node A can only send requests to directly connected peers, B, C, and D, and these nodes will forward the requests. Node D is the target of one request because it is the closest location to the request location.

20. We have explained Freenet operation and FOAF ad infinitum so we will only provide a few sentences that sums up the arguments. The government must have Freenet use even share for their (Levine's) methodology to work. Freenet does not divide requests and share evenly. Freenet uses FOAF routing such that requests are sent toward the node that has the closest location. With FOAF, the number of requests received by any node, from either a relayer or downloader cannot be determined by a connected node and is meaningless. FOAF was activated in Freenet on Sept. 1, 2008, and has been the routing method ever since.

21. The government claims that the Levine test proves their case. We claim the actual Freenet source code proves ours; namely, Freenet uses FOAF routing. (https://github.com/hyphanet/fred/blob/next/src/freenet/node/PeerManager.java#L1042)

22. The government states that Freenet does not work the way the developers intended. This comes from the paper: "Measuring Freenet in the Wild" by Roos, et. al., 2014. We provided this paper as the #2 Exhibit in "Continuation of Exhibits" attached to our Omnibus motion. In this paper they noted that requests took longer to find data than predicted, and this was related to the number of long distance nodes connected versus the short distance nodes. The paper did not state that the FOAF routing was wrong; it just did not work efficiently. As a result, the Freenet developers worked out a fix. Documentation of that fix is provided in Exhibit E with the associated testing. The fix, which was released on 9/23/2014, has been in use with all Freenet releases since that date. The issue referred to by the prosecutor was fixed in 2014, and Freenet operates as the developers intended.
23. At oral argument, the prosecution stated that they would simply bring Dr. Levine who would again state their position. However the government position as stated in the affidavit is even share, and Dr Levine stated in both of the referenced papers that Freenet used FOAF routing. At the Dickerman evidentiary hearing Levine said "***but I'm not trying to estimate how many requests*** *you receive.",* and he described the Freenet routing as: "***They'll look at their collection of -- of peers, their neighbors, and they'll select according to this routing algorithm which one is most likely to have the block from the information they have, and they'll select that one and then they'll pass it on."*** This is FOAF, not even share.

24. There was exculpatory timing data in the FBI spreadsheet. This data is shown below with Dickerman data for comparison.



	Rochester Case			Dickerman Case		
	FOI #1	**FOI #2**	**FOI #3**	**FOI #1**	**FOI #2**	**FOI #3**
Time required to receive requests	3:36:55	2:56:18	0:36:54	0:01:58	0:01:08	0:00:54
Minimum blocks	6374	7690	1847	783	464	623
Maximum blocks	12562	15081	3712	1566	928	1246
Typical blocks - max blocks * .8	10050	12065	2970	1253	742	997
Requests received	69	126	32	69	67	31
Percentage of typical blocks	**0.69%**	**1.04%**	**1.08%**	**5.51%**	**9.02%**	**3.11%**
Average peers of suspect node	69.2	60.4	58.5	56.9	51.1	62.7
% of even-share of min blocks	**74.9%**	**99.0%**	**101.4%**	**501.4%**	**737.9%**	**312.0%**
% of even share of typical blocks	47.5%	63.1%	63.0%	313.4%	461.2%	195.0%

25. This data was taken directly from the FBI spreadsheet or calculated. The timing in the first row is how long it took for the FBI node to receive the requests from a directly connected node (defendant). This shows for file #1 it took over 3 hours and 36 minutes. This is the time to send 69 requests directly to a connected peer. For Dickerman this time was under 2 minutes. The Freenet source code shows that Freenet is sending out messages/requests in 100ms or less (10 requests per second). Since requests are not sent in blocks, or sequentially to a node, the 69 requests should be sent within the time period required to send all 6374 requests. This would be 10.6 minutes, but in this case it took 3 hours and 36 minutes. For comparison to Dickerman, Dickerman would need 1.3 minutes and actually received the data in just under 2 minutes. The data for the other two files is in line with the results for the first file. There is only one explanation for this; that the suspect (defendant's) node was connected to a node which was the actual downloader, and the defendant's node was only relaying the data. The excessive time was due to having an intermediary node. Note that this time is only the time to send a message directly to a connected node, that is, a direct message from A to B. It is not the time to get a response from the network as described in the Roos paper.

26. If you do an internet search for Freenet, https://en.wikipedia.org/wiki/Freenet you find a Wikipedia display that provides an overview of Freenet and references 55 academic papers and articles about Freenet. The point here is that only one article (52) is shown for a Levine reference. That article is the response to the Levine methodology written by the Freenet developers which disputes the validity of the Levine method. There is another article on the Freenet website that also disputes the Levine method but otherwise we could not find any independent analysis of the Levine method. So while we were unable to find other articles that disputed the Levine method, we also found NO articles that validated the Levine method. The academic community seems to have ignored the Levine papers.

Considering Privacy and Fourth Amendment Issues

27. To achieve probable cause in this case the government is attempting to show that the defendant is downloading a file of interest not simply relaying requests from another user for pieces of the file. This is an open net case but it must be pointed out that this does not mean

that the defendant has disclosed his system to the general public. A member of the general public can only see data associated with a Freenet user if they download and install the Freenet software. Even if the Freenet software is installed, the visibility of any node's data is only available to a directly connected node, typically 60 or fewer users (out of 60,000). And even if the directly connected (one of the 60) nodes can see the Freenet user's node, he cannot access that user's computer or download any files or information from it.

28. The Electronic Communications and Privacy Act of 1986 (ECPA) expanded Fourth Amendment privacy protections so oral, wire, and electronic communications are protected equally. Third party doctrine from the 1970's claiming a person has no legitimate expectation of privacy has been superseded by ECPA. Officer Turner's use of customized Freenet software in this case violates all three provisions of ECPA: 18 U.S. Code § 2511 - Interception law; 18 U.S. Code § 2701 - Stored communications law; and 18 U.S. Code § 3121 - Pen register law.

29. Officer Turner had no warrant to intercept or monitor electronic communications pursuant to 18 U.S. Code § 2516. Even service providers are strictly prohibited from monitoring private communications they transmit and may only perform random checks to keep their service working, 18 U.S. Code § 2511(2)(a)(i). For example, phone companies cannot monitor network phone traffic on Mother's Day to predict with 98% accuracy who made calls containing Mother's Day greetings, nor can they analyze who called whom to identify children and their mothers. Phone companies cannot notify police as to who did not call their mother, nor can police tap into the phone network to create such a report without a warrant based on probable cause.

30. Yet, this case involves law enforcement tapping into a private electronic communication network without a warrant and monitoring its communication traffic to predict with 98% accuracy who transmitted particular content, then identifying the person communicating. The same ECPA laws that apply to phone calls, apply to private electronic communications such as file transfers. If no warrant is required, then law enforcement can monitor private communication networks for <u>any</u> content, including Mother's Day greetings or child pornography.

31. Officer Turner was not party to a conversation with Mr. Looney. Instead, Turner's software tapped into Freenet over an internet wire and conducted electronic surveillance of Freenet's communications. (Electronic Surveillance is defined in Executive Order 12333). Then it generated a report read by Officer Turner. **Software is not a person**, so it does not qualify for

the exception "where such person **is** a party to the communication," 18 U.S. Code § 2511(2)(c) and 18 U.S. Code § 2511(2)(d). The present tense of the verb "**IS** a party" requires a person to actively participate in a conversation, not just read a report about it, after the fact.

32. When a regular Freenet user requests a file, he can see only the IP addresses of his immediate peers - 1 hop away. The general public cannot see this information, so these IP addresses are not "publicly available." Freenet communications then hop from peer-to-peer enroute to their destination, up to 18 hops. Communications are temporarily stored on intermediate peers, then forwarded to the next. Temporary electronic storage is defined in 18 U.S. Code § 2510(17)(a). Information about this intermediate network traffic is invisible the owner of that intermediate computer - it is not publicly available. It is this intermediate temporary electronic storage that is analyzed by the customized Freenet software, violating 18 U.S. Code § 2701(a)(2).

33. Officer Turner did not use Freenet as "furnished to the subscriber or user by a provider of wire or electronic communication service," 18 U.S. Code § 2510(5)(a)(i). Instead, he installed a law-enforcement-only version of Freenet on his computer. This version allowed Turner to tap into the internals of Freenet's file transfer system as an intermediate peer and monitor network traffic transmitted over wires and through Turner's computer. Hooking customized software with added wiretapping capability into the Freenet network exceeds the authorization to access the Freenet facility, violating 18 U.S. Code § 2701(a)(2). Officer Turner did not request a file or send an original file, so the exceptions listed in 18 U.S. Code § 2701(c) do not apply.

34. Regular users never see hash codes – they are not publicly available. The wiretapping software extracted and analyzed hash codes, and used a fancy formula to predict with 98% accuracy which IP addresses downloaded child pornography content. "Content" is any information concerning the substance of a communication 18 U.S. Code § 2510(8). Both hash codes and the report generated by the fancy formula qualify as content. "Intercept" means to acquire the content of any electronic communications through the use of any electronic, mechanical or other device, 18 U.S. Code § 2510(4). Officer Turner's affidavit describes in detail how he ascertained that child pornography content was being transmitted and how he acquired this information. But Turner obtained no authorization to intercept content as is required under 18 U.S. Code § 2516. Therefore, this content was unlawfully intercepted, violating 18 U.S. Code § 2511(1)(a). Officer Turner disclosed this unlawfully obtained content to the Court in his

affidavit, violating 18 U.S. Code § 2511(1)(c). The unlawfully obtained content is being used to prosecute Mr. Looney, violating 18 U.S. Code § 2511(1)(d). All unlawfully intercepted content and all evidence derived therefrom should be suppressed, 18 U.S. Code § 2515.

35. Regular users never see the number of times a file piece has been forwarded - this is masked by the non-deterministic nature of whether or not the number is decremented in the initial steps - this is not publicly available. The software records the IP address of the node (directly connected) which sent the request for a file piece based on content and number of times the file piece was forwarded, this IP address is not publicly available. These IP addresses are put into the report.

36. Pen Register / Trap and Trace is not just a device but also a process to record or decode addressing and routing information of electronic communications. An IP address is an address, and it was recorded in the report. The IP address of an intermediate peer also gives a partial description as to the route taken hopping peer-to-peer enroute to the destination. Officer Turner had no pen register / trap and trace warrant to extract addressing or routing information, violating 18 U.S. Code § 3121. Turner submitted administrative subpoenas to decode the identity of the owner from the IP address. Again, Turner had no warrant to decode the IP address and unmask its owner's identity, violating 18 U.S. Code § 3121. The resulting name, John Looney, and the address obtained from the administrative subpoena should be suppressed, 18 U.S. Code § 2515.

Dated: May 17, 2023

Respectfully submitted,

S/James A. Napier, Esq.

James A. Napier, Esq.
Attorney for John Douglas Looney
700 Powers Bldg.
16 W. Main St.
Rochester, New York 14614
585-232-4474
Email:jim@napierandnapier.com

TO: Meghan McGuire, AUSA

CERTIFICATE OF SERVICE

I hereby certify that on May, 17, 2023 , the foregoing was electronically filed with the Clerk of the Court to be served by operation of the Court's electronic filing system upon Ms. Meghan McGuire, Assistant United States Attorney

Attachments

We have attached several documents for the courts information.

A. USAO_000004-000033. The Affidavit in the NYC Case, US v Corbett (29 pgs)

B. Spreadsheet in USA v Corbett case USAO_000034-000034 (1 pg)

C. USAO_000035-000036. Officer's notes in USA v Corbett (2 pgs)

D. USAO_000039-000046. The 2017 Levine Paper (7 pgs)

E. "2014-09-23-Fixing-the-link-length-distribution-in-Freenet". Documentation of the fix that was made by the Freenet developers for the problem noted by the 2014 paper. (12 pgs)

F. "Errors in the Levine 2017 paper on attacks against Freenet with some highlights"- Analysis of Formula by Freenet developer. (11 pgs)